UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/903,612	07/13/2001	Yuri Poeluev	67539/00370	2200

27871 7590 09/19/2006

BLAKE, CASSELS & GRAYDON LLP
BOX 25, COMMERCE COURT WEST
199 BAY STREET, SUITE 2800
TORONTO, ON M5L 1A9
CANADA

EXAMINER	
ABRISHAMKAR, KAVEH	
ART UNIT	**PAPER NUMBER**
2131	

DATE MAILED: 09/19/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/903,612	POELUEV ET AL.	
	Examiner	Art Unit	
	Kaveh Abrishamkar	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 June 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-15* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-15* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. This action is in response to the amendment filed on June 28, 2006. Claims 11-15 are added by virtue of the amendment. Claims 1-15 are currently pending consideration.

Response to Arguments

2. Applicant's arguments with respect to claims 1-15 have been considered but are moot in view of the new ground(s) of rejection.

Claim Objections

3. Claim 10 is objected to because of the following informalities: In the first limitation of the claim 10, "correspondents" is misspelled "respondents." Appropriate correction is required.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the

applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 1-15 are rejected under 35 U.S.C. 102(e) as being anticipated by Ellington, Jr. et al. (U.S. Patent 6,708,218).

Regarding claim 1, Ellington discloses:

A method for providing cryptographic functions to data packets below the network layer of a network stack and transparent to the network layer, the method including the steps of:

intercepting datagrams transferred between the network layer and an other layer below the network layer, said datagrams being encapsulated by a header and footer associated with transfer between the network layer and said other layer and having at least one encapsulated data packet (column 3 lines 29-54, column 7 lines 31-46, column 8 lines 5-8), wherein the IP frames (datagrams) are intercepted and decapsulated;

decapsulating said datagrams by removing said header and said footer to retrieve said at least one encapsulated data packet (column 3 lines 29-54, column 7 lines 31-46, column 8 lines 5-8), wherein the IP frames are decapuslated;

examining said at least one encapsulated data packet and referencing a security policy to determine whether to process said at least one encapsulated data packet according to said security policy using said cryptographic functions (column 3 lines 29-54, column 7 lines 31-46, column 8 lines 5-8), wherein the packet is examined at the

data link layer (MAC header) to determine if the frame is an IPSec frame and if it is, it is processed as such;

if said at least one encapsulated data packet requires processing, modifying said at least one encapsulated data packet to provide said cryptographic functions (column 7 lines 42-46), wherein if it is determined from the MAC header that the data packet is an IPSec frame, then it is placed in a queue which is provided for the packets that require the IPSec processing (cryptographic functions);

reconstructing said datagrams by re-encapsulating said at least one encapsulated data packet with said header and footer for transmission along said network stack (Figure 3, column 2 lines 45-49), where in IPSec the PDU is encapsulated within another IP frame before transmission to the recipient.

Claim 2 is rejected as applied above in rejecting claim 1. Furthermore, Ellington discloses:

The method of claim 1, wherein said data packet is an IP packet having a header, an address and data (column 7 lines 30-40), wherein the packet is an IP packet.

Claim 3 is rejected as applied above in rejecting claim 1. Furthermore, Ellington discloses:

The method of claim 1 wherein said step of modifying said data packet includes the further step of selecting an IPSec protocol (column 7 lines 42-46), wherein if the

packet is determined to be an IP frame requiring IPSec processing it is placed in a special queue, and wherein the IPSec processing can occur in either tunnel or transport mode (column 2 lines 45-55).

Claim 4 is rejected as applied above in rejecting claim 1. Furthermore, Ellington discloses:

The method of claim 1 wherein the step of examining said at least one encapsulated data packet includes the steps of:

checking header information of outbound data packets from said network layer to determine if processing applies (column 8 lines 7-11), wherein the protocol field in the IP header has to be either 50 or 51 for IPSec processing to apply;

checking header information of inbound packets to said network layer to determine if said data packets include cryptographic operations (Figure 9, column 7 lines 47-51), wherein the IP header value is examined on an incoming packet to determine whether or not it is a IPSec frame.

Regarding claim 5, Ellington discloses:

A system for processing data packets for secure communications between correspondents of said system by providing cryptographic functions to data packets below the network layer of a network stack and transparent to the network layer, said system having:

a packet interceptor for intercepting datagrams transferred between the network layer and an other layer below the network layer, said datagrams being encapsulated by a header and footer associated with transfer between the network layer and said other layer and having at least one encapsulated data packet, said packet interceptor for decapsulating said datagrams by removing said header and footer to retrieve said at least one encapsulated data packet, and said packet interceptor for reconstructing said datagrams by re-encapsulating said at least one data packet with said header and footer for transmission along said network stack (column 3 lines 29-54, column 7 lines 31-46, column 8 lines 5-8), wherein the packet is examined at the data link layer (MAC header) to determine if the frame is an IPSec frame and if it is, it is processed as such;

a security policy manager including at least one security policy storing processing rules for said data packets and for selecting at least one of said processing rules for said at least one encapsulated data packet according to said security policy (column 3 lines 29-54, column 7 lines 31-46, column 8 lines 5-8), wherein the packet is examined at the data link layer (MAC header) to determine if the frame is an IPSec frame and if it is, it is processed as such; and

a processing module for examining said at least one encapsulated data packet decapsulated by said packet interceptor, and if said at least one encapsulated data packet requires processing, modifying said at least one encapsulated data packet by selecting and applying said cryptographic functions thereto, said processing module being in communication with said security policy manager (column 7 lines 42-46), wherein if it is determined from the MAC header that the data packet is an IPSec frame,

then it is placed in a queue which is provided for the packets that require the IPSec processing (cryptographic functions);

wherein said datagrams are intercepted and examined in accordance with said processing rules (column 7 lines 42-46), wherein if it is determined from the MAC header that the data packet is an IPSec frame, then it is placed in a queue which is provided for the packets that require the IPSec processing (cryptographic functions).

Claim 6 is rejected as applied above in rejecting claim 5. Furthermore, Ellington discloses:

The system of claim 5, wherein the packet interceptor is a software module located at the data link layer of the network stack (column 7 lines 31-35), wherein the packet is examined at the network stack to see if it requires IPSec processing.

Claim 7 is rejected as applied above in rejecting claim 6. Furthermore, Ellington discloses:

The system of claim 6, wherein said software module is a driver included in a kernel of an operating system in computer readable of said system (column 7 lines 30-41).

Claim 8 is rejected as applied above in rejecting claim 5. Furthermore, Ellington discloses:

The system of claim 5, wherein the cryptographic functions are implemented using an IPSec protocol by said processing module (column 7 lines 42-46), wherein if it is determined from the MAC header that the data packet is an IPSec frame, then it is placed in a queue which is provided for the packets that require the IPSec processing (cryptographic functions).

Claim 9 is rejected as applied above in rejecting claim 5. Furthermore, Ellington discloses:

The system of claim 5, wherein said secure communications between correspondents of said system are provided via a virtual private network (column 3 lines 23-26).

Regarding claim 10, Ellington discloses:

A method for providing a cryptographic system for communication between correspondents in a communication network to data packets below the network layer of a network stack, said method comprising the steps of:

providing a security module in a computer readable medium at each of said correspondents, said security module having:

a packet interceptor for intercepting datagrams between the network layer and an other layer below the network layer, said datagrams being encapsulated by a header and footer associated with transfer between the network layer and said other layer and having at least one encapsulated data packet, said packet interceptor for decapsulating

said datagrams by removing said header and footer to retrieve said at least one encapsulated data packet, and said packet interceptor for reconstructing said datagrams by re-encapsulating said at least one data packet with said header and said footer for transmission along said network stack (column 3 lines 29-54, column 7 lines 31-46, column 8 lines 5-8), wherein the packet is examined at the data link layer (MAC header) to determine if the frame is an IPSec frame and if it is, it is processed as such;

a security policy manager including at least one security policy storing processing rules for said data packets and for selecting at least one processing rule for said encapsulated data packet according to said security policy (column 3 lines 29-54, column 7 lines 31-46, column 8 lines 5-8), wherein the packet is examined at the data link layer (MAC header) to determine if the frame is an IPSec frame and if it is, it is processed as such; and

a processing module for examining said at least one encapsulated data packet decapsulated by said packet interceptor, and if said at least one encapsulated data packet requires processing, modifying said at least one encapsulated data packet by selecting and applying cryptographic functions thereto, said processing module being in communication with said security policy manager (column 7 lines 42-46), wherein if it is determined from the MAC header that the data packet is an IPSec frame, then it is placed in a queue which is provided for the packets that require the IPSec processing (cryptographic functions);

examining said data packets decapsulated by said packet interceptor outbound from said correspondents to determine whether processing by said processing module

is required (column 3 lines 29-54, column 7 lines 31-46, column 8 lines 5-8), wherein the packet is examined at the data link layer (MAC header) to determine if the frame is an IPSec frame and if it is, it is processed as such; and

examining said data packets decapsulated by said packet interceptor inbound to said correspondents to determine whether processing by said processing module is required by checking whether said data packets include cryptographic functions (Figure 9, column 7 lines 47-51), wherein the IP header value is examined on an incoming packet to determine whether or not it is a IPSec frame.

Claim 11 is rejected as applied above in rejecting claim 1. Furthermore, Ellington discloses:

A method according to claim 1 wherein said other layer is the data link layer (column 7 lines 31-36).

Claim 12 is rejected as applied above in rejecting claim 11. Furthermore, Ellington discloses:

A method according to claim 11 wherein said datagrams are PPP datagrams (column 7 lines 31-36), wherein PPP is the standard layer 2 protocol.

Claim 13 is rejected as applied above in rejecting claim 1. Furthermore, Ellington discloses:

A method according to claim 1, said at least one encapsulated data packet being an IP data packet (column 7 lines 30-40), wherein the packet is an IP packet.

Claim 14 is rejected as applied above in rejecting claim 1. Furthermore, Ellington discloses:

A method according to claim 1 wherein said modifying comprises IPSec tunneling (column 7 lines 42-46), wherein if the packet is determined to be an IP frame requiring IPSec processing it is placed in a special queue, and wherein the IPSec processing can occur in either tunnel or transport mode (column 2 lines 45-55).

Claim 15 is rejected as applied above in rejecting claim 1. Furthermore, Ellington discloses:

A method according to claim 1 wherein said referencing comprises reviewing a predetermined set of selectors being one or more of a destination IP address and a transport layer port (column 7 lines 48-55, column 8 lines 1-11).

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kaveh Abrishamkar whose telephone number is 571-272-3786. The examiner can normally be reached on Monday thru Friday 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

KA
09/15/2006

CHRISTOPHER REVAK
PRIMARY EXAMINER

9/16/06